

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-177525

(43) 公開日 平成10年(1998) 6月30日

(51) Int.Cl.⁶

G 0 6 F 12/14

G 0 8 B 25/10

H 0 4 Q 7/38

識別記号

3 2 0

F I

G 0 6 F 12/14

G 0 8 B 25/10

H 0 4 B 7/26

3 2 0 D

Z

1 0 9 R

審査請求 未請求 請求項の数19 O L (全 26 頁)

(21) 出願番号

特願平8-335336

(22) 出願日

平成8年(1996)12月16日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 三浦 興己

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

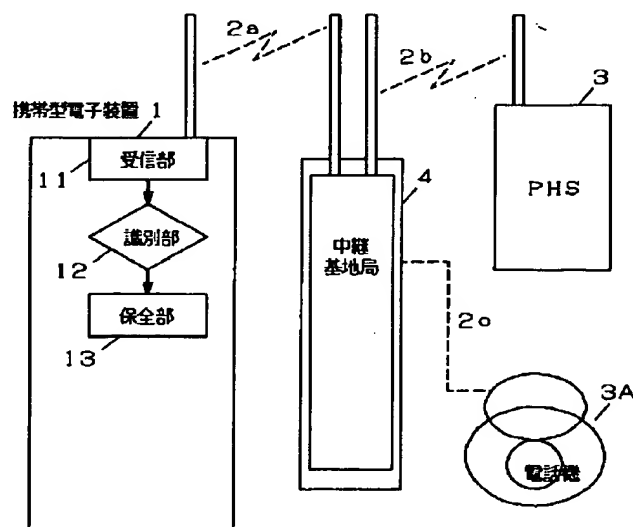
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 携帯型電子装置の保全システム

(57) 【要約】

【課題】 盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除する。

【解決手段】 携帯型電子装置1に電波通信手段を介して送信されてくる遠隔操作データを受信する受信部11と、受信部11で受信した遠隔操作データを識別する識別部12と、識別部12による識別結果に基づいて携帯型電子装置1の所有者が害を被ることを排除する所定の保全部13を設け、携帯型電子装置1が盗まれたり紛失した場合に、ネットワークやオンラインシステムの回線事業会社に連絡して回線の解約解除の手続きをする前に、保全部13で保全処理することにより、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを可能にする。



【特許請求の範囲】

【請求項1】 携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設け、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを特徴とする携帯型電子装置の保全システム。

【請求項2】 携帯型電子装置が盗まれたり紛失した時に電波通信手段を介して送信されてきた遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたことを特徴とする請求項1記載の携帯型電子装置の保全システム。

【請求項3】 電波通信手段を介して送信されてくる遠隔操作データを受信し、該遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を1つまたは1つ以上設けたことを特徴とする請求項2記載の携帯型電子装置の保全システム。

【請求項4】 保全処理手段は、携帯型電子装置の所有者が予め入力したキーワードを記憶する第1記憶手段と、電波通信手段を介して送信される遠隔操作データを受信し、該遠隔操作データの識別結果のキーワード情報を記録する第2記録手段、前記第1記憶手段のキーワードと前記第2記録手段のキーワード情報との一致を確認した後、保全処理を実行することを特徴とする請求項2または3記載の携帯型電子装置の保全システム。

【請求項5】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項6】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項7】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に記憶した連絡先やメッセージを表示し、携帯型電子装置を回収する「メッセージ表示」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項8】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に記憶した連絡先のみにのみ交信する「所有者連絡

発信」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項9】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の本来の機能のうち所有者が予め入力した機能を停止する「発信機能禁止」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項10】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項11】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項12】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項13】 保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項14】 保全処理手段の保全処理内容として、使用者の識別手段により使用者を識別し、所有者以外の他人が携帯型電子装置の使用を不可能にする「保全処理」を行うことを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項15】 送信した相手または相手情報に対する保全処理手段は、遠隔操作データによって、

a. 携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理と、

b. 携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理と、

c. 携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理と、

d. 携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理と、

e. 携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理と、

f. 携帯型電子装置に送信した相手に、該携帯型電子装置の保全システムの使用を防止する保全処理と、のうち1つ以上の処理を実施することを特徴とする請求項3記載の携帯型電子装置の保全システム。

【請求項16】 電波通信手段を伝送媒体にして、所有者が予め入力して記憶手段に記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全処理手段を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことを特徴とする請求項5乃至14の何れかに記載の携帯型電子装置の保全システム。

【請求項17】 所有者が予め入力して記憶手段に記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置を接続し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことを特徴とする請求項5乃至14の何れか1項に記載の携帯型電子装置の保全システム。

【請求項18】 携帯型電子装置に保全処理を促すための発振手段、該発振手段の発振信号を送信する微弱電力送信手段を有する携帯型電子装置の子機と、該子機からの保全処理を促すための発振データを受信する微弱電力受信手段、該微弱電力受信手段で受信した操作データを識別する識別手段、該識別手段の識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を揺する本体を備え、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを特徴とする携帯型電子装置の保全システム。

【請求項19】 携帯型電子装置との間で交信する微弱電力伝送手段、該微弱電力伝送手段の受信信号から携帯型電子装置との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を促すための発振データを前記微弱電力伝送手段で受信し、該発振データにより警告音を発生する手段を有する携帯型電子装置の子機と、前記子機と同様の双方の微弱電力伝送手段、子機との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を起動し、警告音を発生する手段を有する本体を備え、紛失あるいは盗難および置き忘れを防止することを特徴とする携帯型電子装置の保全システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯型電子装置（PHS、携帯電話機も含む電波通信手段を有するデータ処理端末装置をいう）の盗難や紛失に対して所有者が害を被ることを排除し、所定のセキュリティを高める保全処理機能を備えた携帯型電子装置の保全システムに関する。

【0002】

【従来の技術】従来、上記のような携帯型電子装置は、その装置の特色上、広い不特定領域の屋外に持ち出して使用される。また、通信回線を登録した携帯型電子装置は、PHS（Personal Handy Phone System）、そのデータ処理端末装置などデジタル信号情報のコンピュータ

周辺端末装置として用途が拡大するとともに、その持ち出し使用領域を広げていくことができる。また、その使用方法も容易で、多くの人々の需要がある。

【0003】

【発明が解決しようとする課題】しかしながら、この種従来の携帯型電子装置は、所有者がその装置自体を屋外などに持ち出して使用したり、手軽に携帯できるため、盗難や紛失する機会が多く、盗難や紛失したこの種の携帯型電子装置を他人が拾得した場合にも、容易に使用できる可能性があり、元々の所有者はプライベート情報や重要データを盗み見されたり、使用していない通話料金などの請求を請けるなど所有者が害を被る問題が発生している。

【0004】また、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思って送信したことで、送信相手または相手情報が害を被る問題が発生するおそれもある。

【0005】本発明は、このような従来の問題点を解決するものであり、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除できる携帯型電子装置の保全システムを提供することを目的とするものである。

【0006】

【課題を解決するための手段】この課題を解決するために本発明は、携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設けたものである。

【0007】これにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除できる。

【0008】

【発明の実施の形態】本発明の請求項1に記載の発明は、携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能になる。

【0009】本発明の請求項2に記載の発明は、携帯型電子装置が盗まれたり紛失した時に電波通信手段を介して送信されてきた遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手

者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能となる。

【0010】本発明の請求項3に記載の発明は、電波通信手段を介して送信されてくる遠隔操作データ受信し、該遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を1つまたは1つ以上設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能となる。

【0011】本発明の請求項4に記載の発明は、保全処理手段が、携帯型電子装置の所有者が予め入力したキーワードを記憶する第1記憶手段と、電波通信手段を介して送信される遠隔操作データを受信し、該遠隔操作データの識別結果のキーワード情報を記録する第2記録手段、前記第1記憶手段のキーワードと前記第2記録手段のキーワード情報との一致を確認した後、保全処理を実行することにより、携帯型電子装置を使用する折に、個々のキーワードを入力しなければ動作せず、所有者の大切な登録情報を保全・安全・確実を保証するセキュリティが保たれ、個別のキーワードの適用により厳格に守る仕組みが成り立ち、盗難や紛失での管理作業での誤りを生ずることが回避でき、登録情報やその管理のセキュリティを高めることができる。

【0012】本発明の請求項5に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理を行うことにより、電源が入らなくなるので携帯型電子装置の基本機能を殺す保全処理がなされ、携帯型電子装置の紛失者にとって最小限の損失に抑えることができる。

【0013】本発明の請求項6に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理を行うことにより、携帯型電子装置の拾得者に警告発生することで携帯型電子装置の使用を禁止する保全処理が可能になり、携帯型電子装置の紛失者にとって他人に使用することを防止できる。

【0014】本発明の請求項7に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に記憶した連絡先やメッセージを表示し、携帯型電子装置を回収する「メッセージ表示」の保全処理を行うことにより、携帯型電子装置の拾得者にメッセージ表示するから、携帯型電子装置の返却を訴える保全処理が可能になり、携帯型電子装置の紛失者にと

って他人に使用することを防止でき、携帯型電子装置の返却が可能になる。

【0015】本発明の請求項8に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に記憶した連絡先のみと交信する「所有者連絡発信」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し所有者連絡発信で連絡が取れるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、携帯型電子装置の返却が可能になる。

【0016】本発明の請求項9に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の本来の機能のうち所有者が予め入力した機能を停止する「発信機能禁止」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し発信機能禁止ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【0017】本発明の請求項10に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を保護するデータ出力禁止がかかるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【0018】本発明の請求項11に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を保護する記憶データ消去ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できるほか、個人データや情報を悪用されることを阻止できる。

【0019】本発明の請求項12に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し通信回線番号消滅ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避することができる。

【0020】本発明の請求項13に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を遠隔操作でデータ転送できるから、携帯型電

子装置内の個人データや情報を回収でき、携帯型電子装置内の記憶データを消去できるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【0021】本発明の請求項14に記載の発明は、保全処理手段の保全処理内容として、使用者の識別手段により使用者を識別し、所有者以外の他人が携帯型電子装置の使用を不可能にする「保全処理」を行うことにより、携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることを排除する所定のセキュリティを高め得る。

【0022】本発明の請求項15に記載の発明は、送信した相手または相手情報に対する保全処理手段は、遠隔操作データによって、a. 携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理と、b. 携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理と、c. 携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理と、d. 携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理と、e. 携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理と、f. 携帯型電子装置に送信した相手に、該携帯型電子装置の保全システムの使用を防止する保全処理のうち1つ以上の処理を実施することにより、携帯型電子装置が盗難や紛失された場合には、携帯型電子装置の保全システムの所有者が予め入力したキーワードを蓄積記憶させておき、電波通信を媒体にし遠隔操作でそのキーワードデータを他の電送装置から送信すると、キーワード情報との一致を確認した後で、保全処理を実行することができ、所有者の大切な登録情報を保全・安全・確実に保証するセキュリティが保たれるものであり、盗難や紛失しても他人に悪用される危険を回避できる。

【0023】本発明の請求項16に記載の発明は、電波通信手段を伝送媒体にして、所有者が予め入力して記憶手段に記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全処理手段を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことにより、携帯型電子装置の紛失者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信し、強制的に携帯型電子装置の保全機能を駆動し、装置の紛失者にとって他人に使用されることを防止できる。

【0024】本発明の請求項17に記載の発明は、所有者が予め入力して記憶手段に記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置を接続し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことにより、携帯型電子装置の拾得者が応

答しなとか、交信ができない事態の場合においても、呼び出し信号回数のパターンによる遠隔保全処理を起動させ、装置の紛失者にとって他人に使用されることを防止できる。

【0025】本発明の請求項18に記載の発明は、携帯型電子装置に保全処理を促すための発振手段、該発振手段の発振信号を送信する微弱電力送信手段を有する携帯型電子装置の子機と、該子機からの保全処理を促すための発振データを受信する微弱電力受信手段、該微弱電力受信手段で受信した操作データを識別する識別手段、該識別手段の識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を揺する本体を備えることにより、未然に紛失または置き忘れを防止し回避することができ、また所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【0026】本発明の請求項19に記載の発明は、携帯型電子装置との間で交信する微弱電力伝送手段、該微弱電力伝送手段の受信信号から携帯型電子装置との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を促すための発振データを前記微弱電力伝送手段で受信し、該発振データにより警告音を発生する手段を有する携帯型電子装置の子機と、前記子機と同様の双方の微弱電力伝送手段、子機との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を起動し、警告音を発生する手段を有する本体を備えることにより、携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置の保全システムを容易に実施することができ、携帯型電子装置を紛失または置き忘れを防止できる。

【0027】以下、本発明の実施の形態について、図面を参照して説明する。

(実施の形態1) 図1は、本発明の請求項1に対応する実施の形態1における携帯型電子装置の保全システムの構成図である。同図において、1は例えばPHS(Personal Handy Phone System)データ通信装置や携帯電話としての携帯型電子装置、2a, 2b, 2cは公衆回線網などに接続された通信回線などの電波通信手段、3は公衆回線網などに接続された一般公衆電話や携帯電話としてのPHSなど電話機、4は中継基地局である。更に電話機3Aは公衆回線網などに接続された中継基地局4から無線通信回線2bを介した別のPHSデータ通信装置や携帯電話としてのPHSを構成する。

【0028】携帯型電子装置1は、電波通信手段2aを伝送媒体にし遠隔操作データを受信する受信部11、受信した遠隔操作データを識別する識別部12、この識別部12の識別結果により携帯型電子装置1の所有者が害

を被ることを排除する所定の保全部 13 を備え、携帯型電子装置 1 の所有者の財産または情報に関わるセキュリティを行い、携帯型電子装置所有者の財産または情報を保全する。

【0029】市内や市外の一般公衆電話 3 から公衆回線網 2b を介して、また PHS データ通信装置や携帯電話としての PHS 3A から無線通信回線 2c を介して保全を要する携帯型電子装置 1 に遠隔操作データを送信する。該携帯型電子装置 1 は該遠隔操作データを受信部 11 で受信し、受信した遠隔操作データが予め記憶された所定の遠隔操作データと一致したかを識別部 12 が判別する。識別部 12 では、その識別結果により一致が確認された場合のみ保全部 13 が携帯型電子装置 1 の所有者が害を被ることを排除するために所定の保全処理を行う。

【0030】次に、図 4 は携帯型電子装置のネットワークシステムを示す構成図であり、公衆ならびに専用回線網 30 には、交換機を介して一般の電話機 31 が接続されているとともに、変復調器 (MODEM) 付きのパソコン 32、携帯型電子装置の多数の基地局 33～35 および網管理局 36 が接続される。多数の基地局 33～35 には個々の携帯型電子装置が無線通信回線を介し接続される。例えば、基地局 33 には無線通信回線を介して携帯型パソコン、無線通信パソコン、無線通信電子手帳が接続され、基地局 34 は無線通信回線を介して携帯型電話機、PHS、目線通信機が接続され、基地局 35 は無線通信回線を介して携帯型情報端末機が接続されている。また、網管理局 36 は網全体を制御し管理するもので、各端末に対しての制御を行なう。

【0031】個々の携帯型電子装置は保全機能を備えており、この保全機能は、その所有者より送信された遠隔操作データを受信した場合、この遠隔操作データに基づいて携帯型電子装置の所有者に不利益になる要因を排除する所定の保全処理を実行するための制御や、キーワードの入力や解析処理を実施するための制御を行ない、また異なった入力に対しても設定された保全処理を実施するための制御を行う。

【0032】したがって、本発明の実施の形態 1 では、携帯型電子装置は電波通信手段と伝送媒体を通して遠隔操作データを受信部 11、受信した遠隔操作データを識別する識別部 12、この識別部 12 の識別結果により携帯型電子装置の所有者が害を被ることを排除する保全部 13 により、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることができるという効果がある。

【0033】(実施の形態 2) 図 2 は、本発明の請求項 2 に対応する実施の形態 2 における携帯型電子装置の保全システムの構成を示す、例えば PHS 端末の機能ブロック図であり、キー基板と RF 基板で構成される。同図において、モデム部 221 は、音声符号をの適応予測と

適応量子化により圧縮／伸張する ADPCM コーディック 2211、バッファ 2212、フレームプロセッサ 2213、 $\pi/4$ QPSK 変調器 2214 及び $\pi/4$ QPSK 復調器 2215 を備え、ADPCM コーディック 2211 には PCM コーディック 228 を介してスピーカ 233 及びマイク 234 が接続されている。また、235 はバッテリー、236 は電圧安定器、237 は各回路へ電源を供給する電源回路である。

【0034】プロトコル・プロセッサ部 230 は、所定のプロトコルに従い携帯型電子装置を制御するもので、CPU とメモリ等から構成される。図 3 はプロトコル・プロセッサ部の構成を示している。同図において、プロトコル・プロセッサ部 230 は、CPU (制御部) 2301、プロトコル・プロセッサ 2302、カレンダー時計、タッチパネル、表示部 I/F、赤外線 I/F、シリアル I/F、PC カード I/F、音声発生 I/F、各種センサ I/F、各種入力 I/F 等に対するマンマシン I/F プロセッサ 2303、RAM、ROM、F-ROM の相当するメモリ 2304、保全処理部 2305、発信機能、送信機能、転送機能を発揮するプロトコルプロセッサ 2306、RF コントローラ 2307 及び電源制御部 2308 を備え、マンマシン I/F プロセッサ 2303 にはキーパッド 231 及び LCD ドライブ 232 が接続されている。

【0035】この構成において、無線送受信部はアンテナ 201 に到来する電波を受信側に選択された送受信切替用の FET スイッチ 202 を経由し、受信帯域のバンドパスフィルタ (BPF) 203 で選択された後、LNA (ローノイズアンプ) 204 で増幅される。この LNA 204 にはアッテネータが内蔵され、強電界での信号入力時にはアッテネータに切り換えることによって受信回路の飽和を防ぎ広いダイナミックレンジを確保する。LNA 204 で増幅された信号は、送受信切替用の FET スイッチ 205 を介して、もう 1 段のバンドパスフィルタ (BPF) 206 に送出され、この BPF 206 でイメージなどの不要電波を除去した後、送受信切替用の FET スイッチ 207 を介して第 1 ミキサ 208 へ送られる。

【0036】第 1 ミキサ 208 では、受信信号と、発振部 (TCXO) の発振信号を基にシンセサイザ 210 からアンプ 211 を通して得られる第 1 ローカル信号とをミキシングし、周波数チャネルの選択を行なうとともに 248.45MHz の中間周波数へ変換する。このミキサ 208 は相互変調による耐妨害特性を高めるため、高いインターセプトポイントを有する。ミキサ 208 の出力は、送受信切替用の FET スイッチ 212 を介して狭帯域フィルタ特性の SAW フィルタ (BPF) 213 を経由して出力される。この SAW フィルタ 213 は隣接チャネルの選択度およびイメージ妨害特性を決定し、同時に優れた群遅延特性を有する。SAW フィルタの代用として

アナログコードレス用のヘリカルフィルタを使用した場合は、イメージ周波数のみ減衰させ、次段の中間周波数で除去する。

【0037】SAWフィルタ213を通過した信号は送受信切替用のFETスイッチ214を介して第2ミキサ215に入力され、ローカル発振器218からの信号とミキシングすることにより10.75 MHzに変換させる。第2イメージ妨害はSAWフィルタ213の能力のみで決まるため、第2ミキサ215はイメージリジクトタイプのものである。これによりSAWフィルタ213のイメージ除去能力は緩和する。10.75 MHzのIF信号はバンドパスフィルタ(BPF)216通過した後、第3ミキサ217でローカル発振器218からの信号とミキシングされ、さらにバンドパスフィルタ(BPF)219を通過させることで1.15MHzに変換する。そして、リミッタ220で検出された信号はモデム部221に送られる。

【0038】一方、モデム部221の $\pi/4$ QPSK変調器2214で作られた $\pi/4$ QPSK変調波は、デジタルデータとして図示省略のD/Aコンバータに入力される。D/Aコンバータでは10.75 MHzの変調波となり、バンドパスフィルタ(BPF)222で不要信号が除去される。10.75 MHzのIF信号は送信用ミキサ223に入力され、ローカル発振器218からの信号とミキシングすることにより248.45MHzに変換される。この送信側のIF信号は受信と共用したSAWフィルタ213を通すことによりイメージなどの不要信号を除去した後、送受信切替用のFETスイッチ212及びパワー調整部224を介して送信用ミキサ225へ入力される。このミキサ225はシンセサイザ210からの第1ローカル信号とミキシングされ、送信周波数に変換する。この信号は、受信と共用する帯域通話フィルタ206を通してパワーアンプ226に入力される。このパワーアンプ226では必要なパワーに信号を増幅し、増幅された信号はローパスフィルタ(LPF)227で高周波分が除去され、送信切替用のFETスイッチ202を経由してアンテナ201から放射される。

【0039】一方、マイク234から入力された音声信号はPCMコーデック228でデジタル化され、64 Kbpsで入力されるPCM信号をADPCMコーデック2211でADPCM変換(圧縮)し、32Kbpsのデータにする。このデータは一旦バッファ2212に一時記憶させた後、フレームプロセッサ2213でTDMAフレームに構成する。このときにユニークワード、CI、SA、CRC等の付加情報が加わるため、384 Kbpsまでデータレートは増加する。このデータを $\pi/4$ QPSK変調器2214で10.75 MHzの変調波として図示省略のD/Aコンバータに入力する。一方、1.15MHzの受信データは $\pi/4$ QPSK復調器2215で検波され、ADPCMコーデック2211で64Kbpsに伸張され、PCM

コーデック228でD/A変換されてスピーカ233へ出力される。その他に、送信/受信の切り替えタイミングの制御、RSSIの検出判定、AFC制御やシンセサイザデータの設定、及び無線系のコントロールを行う。また、本実施の形態2の場合、遠隔操作データを受信した時には、この受信した遠隔操作データに基づき携帯型電子装置の所有者が害を被ることを排除する保全処理部2305を制御し、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高める保全処理を実行すべき制御を行う。

【0040】次に、携帯型電子装置の所有者が携帯型電子装置を盗まれたり紛失した場合について述べる。この場合は、図5に示すセキュリティを高める保全処理の制御ルーチンを実行する。まず、ステップS10において、携帯型電子装置の所有者は網管理局36に対して変復調器(MODEM)を介しパソコン32を用いて所有する携帯型電子装置に対して通信を開始すべく遠隔操作データを入力する。この場合、携帯型電子装置が携帯していない状況(盗難や紛失)および内部に記憶されている情報の重要度により送信する遠隔操作データの内容を選択する。遠隔操作データには制御コードが所有者のみが事前に付加しており、所有者のみが知っているキーワードがある。したがって、所有者以外の例えば拾得者が任意に所有者の携帯型電子装置に対して遠隔操作データを送ることや解除することはできない。これにより遠隔操作の悪用を防止できる。

【0041】また、携帯型電子装置のネットワークシステムで、携帯型電子装置の所有者がパソコン32を保有していないような場合、または保有していても網管理局36に対して変復調器(MODEM)を介し駆動するシステムになっていない時は、公衆回線網30の一般の電話機31により携帯型電子装置の基地局34に遠隔操作データの送信を依頼する。またはプッシュ回線により遠隔操作データを入力する。

【0042】次のステップS11では、携帯型電子装置の所有者が入力した遠隔操作データを公衆ならびに専用回線網30を介して携帯型電子装置の基地局34に転送する。次のステップS12では、携帯型電子装置の基地局34より無線で遠隔操作データを送信する。

【0043】以上のようにパソコン32より入力した遠隔操作データが公衆ならびに専用回線網30を介して携帯型電子装置の基地局34に送られ、目的の所有者の手元のない所有者の携帯型電子装置に送信される。なお、携帯型電子装置が双方向二重通損の機能を有しておれば、リンクが確立し所有者の操作するパソコン32へ携帯型電子装置の受信が確実に実行されたことを伝送する。

【0044】したがって、本実施の形態2では、電波通信手段を伝送媒体にし受信した遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排

除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高める得る効果がある。

【0045】（実施の形態3）次に、携帯型電子装置の所有者がその装置を盗まれたり紛失して、該携帯型電子装置を他人が拾得した場合に発生しうる問題は、元々の所有者はプライベート情報や重要データを盗み見されたり、使用していない通話料金などの請求を請けるなど該携帯型電子装置の所有者が害を被る問題と、盗難や紛失した携帯型電子装置の所有者に送信した相手にとって、不適切な状況であることを知らずに携帯型電子装置の所有者と誤って送信したことで、送信相手または相手情報が害を被る問題がある。

【0046】したがって、請求項3に対応する本実施の形態3では、携帯型電子装置の所有者が、その携帯型電子装置を盗まれたり紛失した場合は、図5に示すセキュリティを高める保全処理の制御ルーチンを実行する。ステップS10において、携帯型電子装置の所有者は網管理局36に対して変復調器（MODEM）を介しパソコン32を用いて所有する携帯型電子装置に対して通信を開始すべく遠隔操作データを入力する。この場合に携帯型電子装置が携帯していない状況（盗難や紛失）および内部に記憶されている情報の重要度により送信する遠隔操作データの内容を選択する。遠隔操作データには制御コードが事前に付加されており、この制御コードは所有者のみが知っているキーワードある。

【0047】そこで、電波通信手段を伝送媒体にしてデータ受信した遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を備える携帯型電子装置において、送信した相手または相手情報が害を被るのを防止するための保全処理手段では、携帯型電子装置の所有者が予め記憶手段に記憶しておいたキーワードと、電波通信手段を媒体にし遠隔操作データを受信した時の識別結果のキーワード情報との一致を確認した後に、後述する実施の形態15で説明する各保全処理を実行する。

【0048】すなわち、遠隔操作データによって、

- a. 携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理、
- b. 携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理、
- c. 携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理、
- d. 携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理、
- e. 携帯型電子装置に送信した相手に、所有者があらかじめ入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理、
- f. 携帯型電子装置に送信した相手に、該携帯型電子装

置の使用を防止する保全処理、のうち1つ以上の処理を実行する。

【0049】したがって、本実施の形態3では、盗まれたり紛失した携帯型電子装置の所有者に送信した相手にとって、送信相手の携帯型電子装置が不適切な状況にあることを知り、保全処理することによって送信相手または相手情報が害をこうむるのを防止することができる。

【0050】（実施の形態4）携帯型電子装置の所有者が、その携帯型電子装置を盗まれたり紛失した場合に、上記図5に示すセキュリティを高める保全処理の制御ルーチンのようにキーワードと遠隔操作データが所有者の手元になく所有者の携帯型電子装置に送信されると、該携帯型電子装置の保全処理手段は図6に示す遠隔操作データの処理ルーチンを実行する。以下、その処理ルーチンについて図6を参照して説明する。

【0051】図6において、ステップS20では、紛失の携帯型電子装置がキーワードと遠隔操作データを受信し、次のステップS21において、遠隔操作のキーワードが予め所有者が記憶手段に記憶しておいたキーワードであるか否かを識別する。ここで、不一致である場合は保全処理システムを終了し、通常モードに戻る。また、キーワードが一致した場合は保全処理システムを立ち上げ、装置のプロテクト機能を起動する。その後、遠隔操作データであるか否かを識別する。ここで、遠隔操作データでない場合は保全処理システムを終了し、通常モードに戻る。また、遠隔操作データである場合はステップS22に進み、遠隔操作データの保全内容を解析する。

【0052】遠隔操作データは各保全処理にコードが予め定められており、例えば「警告発生」、「メッセージ表示」、「所有者連絡発信」、「発信機能禁止」、「データ出力禁止」、「記憶データ消去」、「通信回線番号消滅」、「電源オフ」など、所定のコードにより分岐し、個々の保全処理ルーチンに進む。

【0053】すなわち、ステップS23では、遠隔操作データの内容が「警告発生」コードと一致すると判別した場合はステップS24に進み、「警告発生」の保全処理を実行する。ステップS23で不一致の場合は次の処理コードのステップS25に進み、次々と一致するコードを検索して進む。その他の遠隔操作データの内容においても同様であり一致した場合には該当した保全処理を実行する。非該当のコードであれば保全処理システムを終了する又は固定の保全処理をする。

【0054】次にステップ25では、遠隔操作データの内容が「メッセージ表示」コードと一致するか否かを識別し、一致した場合にはステップS26に進み、「メッセージ表示」の保全処理を実行する。ステップS25で不一致の場合は次の処理コードのステップS27に進む。ステップS27では、遠隔操作データの内容が「発信機能禁止」コードと一致するか否かを識別し、一致し

た場合はステップS 2 8に進み、「発信機能禁止」の保全処理を実行する。ステップS 2 7で不一致の場合は次の処理コードのステップS 2 9に進む。

【0055】ステップS 2 9では、遠隔操作データの内容が「所有者連絡発信」コードと一致するか否かを識別し、一致した場合はステップS 3 0に進み、「所有者連絡発信」の保全処理を実行する。ステップS 2 9で不一致の場合には次の処理コードのステップS 3 1に進む。

【0056】次にステップS 3 1では、遠隔操作データの内容が「記憶データ消去」コードと一致するか否かを識別し、一致した場合にはステップS 3 2に進み、「記憶データ消去」の保全処理を実行する。ステップS 3 1で不一致の場合は次の処理コードのステップS 3 3に進む。ステップS 3 3では、遠隔操作データの内容が「データ出力禁止」コードと一致するか否かを識別し、一致した場合はステップS 3 4に進み、「データ出力禁止」の保全処理を実行する。ステップS 3 3で不一致の場合は次の処理コードのステップS 3 5に進む。

【0057】ステップS 3 5では、遠隔操作データの内容が「通信回線番号消滅」コードと一致するか否かを識別し、一致した場合はステップS 3 6に進み、「通信回線番号消滅」の保全処理を実行する。ステップS 3 5で不一致の場合は次の処理コードのステップS 3 7に進む。ステップS 3 7では、遠隔操作データの内容が「記憶データ転送」コードと一致するか否かを識別し、一致した場合にはステップS 3 8に進み、「記憶データ転送」の保全処理を実行する。ステップS 3 7で不一致の場合は次の処理コードのステップS 3 9に進む。ステップS 3 9では、遠隔操作データの内容が「使用者の識別」コードと一致するか否かを識別し、一致した場合はステップS 4 0に進み、「使用者の識別」の保全処理を実行する。ステップS 3 9で不一致の場合は次の処理コードのステップS 4 1に進む。

【0058】ステップS 4 1では、遠隔操作データの内容が「電源オフ」コードと一致するか否かを識別し、一致した場合はステップS 4 2に進み、「電源オフ」の保全処理を実行する。ステップS 4 1で不一致の場合は次の処理コードのステップS 4 3に進み、どのコードにも非該当のコードであれば、ステップS 4 5で保全処理システムを終了する。又はステップS 4 4で固定の保全処理として例えば「電源オフ」の保全処理を実行して終了する。

【0059】上記の説明のように本実施の形態4では、携帯型電子装置は携帯型電子装置の所有者が予め入力したキーワードを記憶手段に記憶しておき、電波通信手段を媒体にして遠隔操作データを受信し、その識別結果の保全処理コード情報を記録手段に記録し、この記憶手段のキーワードと保全処理コード情報との一致を確認した後で、図6に示す処理を実行することで、携帯型電子装置の保全を実現できるとともに、ケースバイケー

スで最適の保全処理を選択し、最適の運用を適用することができる効果がある。

【0060】（実施の形態5）本発明の実施の形態5における保全処理手段の保全処理内容aについて、図7を参照して説明する。

【0061】保全処理内容aは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理である。

10 【0062】図7は携帯型電子装置の本来の機能を停止するための「電源オフ」の保全処理ルーチンを示すフローチャートである。まず、ステップS 4 4 1において「電源オフ」フラグがオンかを判定し、「電源オフ」フラグがオンでない場合はステップS 4 4 2に進み、「電源オフ」の保全処理を実行しない。また、「電源オフ」フラグがオンである場合はステップS 4 4 3に移行してパワーオンスイッチ・ディスエーブルフラグをオンする。そして、ステップS 4 4 4で携帯型電子装置の電源を強制的にオフし、「電源オフ」の保全処理を実施し（ステップS 4 4 5）、電源オンを禁止する命令が優先的に実行される。

20 【0063】このように、遠隔操作データで「電源オフ」保全処理をした場合、マニュアルモードにして携帯型電子装置の電源スイッチをオンしても、制御部はパワーオンシーケンスでフラグがオンを確認し、電源をオフに移行させる。従って、携帯型電子装置の電源がオンにならないので、例えば盗難に遭遇したような場合であっても他人に使用されず、回線使用料金が無謀に請求されることがない。

30 【0064】この「電源オフ」保全処理は、携帯型電子装置の電源スイッチをオフにしてしまうもので、手順上極めて明解な保全処理であり、所有者が携帯型電子装置を盗まれたり紛失したことに気が付いた場合において、以下に示す保全処理内容b～jなどで処理できなかった折に最終的に施す保全処理として活用するのに適している。更に他の保全処理内容b～jなどで処理した後、「電源オフ」の保全処理を複合させて活用するようにしてもよい。

40 【0065】また、「電源オフ」保全処理は、携帯型電子装置の本来の機能を停止することを目的にするもので、上記のパワーオンスイッチ・ディスエーブルフラグをオンする以外の手段で、マイクロコンピュータのリセットオンや駆動用発振機能オフなどの手段などあらゆるハード手段も含むものである。

【0066】多くの保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

50 【0067】特に、本実施の形態5では、電源が入らな

いので装置の基本機能を殺す保全処理により、装置の紛失者にとって最小限度の損失に抑えることができる。

【0068】（実施の形態6）本発明の実施の形態6における保全処理手段の保全処理内容bについて、図8を参照して説明する。

【0069】保全処理内容bは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理である。例えば、置き忘れや紛失された携帯型電子装置の表示部に所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示すること、またはスピーカから呼び掛けを音声を発信することにより、拾得者から所有者への返還を容易にする。

【0070】図8は携帯型電子装置の本来の機能を停止するための「警告発生」の保全処理ルーチンを示すフローチャートである。「警告発生」の保全処理ルーチンでは、まず、ステップS241において「警告発生」フラグがオンかを判定し、「警告発生」フラグがオンでない場合はステップS242に進み、「警告発生」の保安処理を実行しない。また、「警告発生」フラグがオンである場合はステップS243に移行してスピーカからアラーム音を発生させ、また液晶などの表示部の全面を点滅させる（ステップS244）。そして、アラーム音の発生時間及び表示部の表示時間をカウントし（ステップS245）、所定時間経過したかを判定する（ステップS246）。ここで、所定時間経過しない場合はステップS243に戻り、所定時間経過した場合はステップS241に戻る。

【0071】このように、例えば盗難や紛失に遭遇したような場合であっても他人がアラーム音を止めることができず、表示部の点滅の繰り返し表示を止めることができない。したがって、紛失した場合に第3者に発見し拾得しやすく、拾得者が使用することを防止し所有者に返還させる。

【0072】ただし、警告音や表示部の点滅の繰り返しは、携帯型電子装置の電池の消費電力が大きいため、第3者に発見されずに電池の消耗になる恐れがあるので、一定時間のみ駆動させる。

【0073】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【0074】特に、本実施の形態では、装置の拾得者により警告発生により装置の他人使用の禁止を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、併せて所有者に返還させる効果大きい。

【0075】（実施の形態7）本発明の実施の形態7における保全処理手段の保全処理内容cについて、図9を参照して説明する。

【0076】保全処理内容cは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め記憶手段に蓄積記憶した連絡先やメッセージを呼び掛け表示し、装置を回収する「メッセージ表示」の保全処理である。例えば、盗まれたり紛失した携帯型電子装置の所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示部に表示すること、またはスピーカから呼び掛けをすることにより、拾得者が使用することを防止したり、所有者に返還させる。

【0077】図9は携帯型電子装置の本来の機能を停止するための「メッセージ表示」保全処理のルーチンを示すフローチャートである。まず、ステップS261において「メッセージ表示」フラグがオンかを判定し、

「メッセージ表示」フラグがオンでない場合はステップS262に進み、「メッセージ表示」の保安処理を実行しない。また、「メッセージ表示」フラグがオンである場合はステップS263に移行してメッセージコード番号によりメッセージ内容を選択し、記憶した所定の表示内容1を表示部に表示する（ステップS264）。そして、記憶した所定の呼び掛け音1をスピーカから発生させ（ステップS264A）、メッセージ表示の保全処理を実施する（ステップS267）。

【0078】また、メッセージコード番号により別のメッセージ内容を選択した場合は、記憶した所定の表示内容2を表示部に表示する（ステップS265）。そして、記憶した所定の呼び掛け音2をスピーカから発生させ（ステップS265A）、メッセージ表示の保全処理を実施する（ステップS267）。また、メッセージコード番号により更に別のメッセージ内容を選択した場合は、記憶した所定の表示内容3を表示部に表示する（ステップS266）。そして、記憶した所定の呼び掛け音3をスピーカから発生させ（ステップS266A）、メッセージ表示の保全処理を実施する（ステップS267）。

【0079】このように「メッセージ表示」の保全処理のルーチンでは、メッセージ表示フラグをオンすると事前に記憶した所定の表示内容が液晶などの表示部に表示できるから、携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に蓄積記憶した連絡先やメッセージが表示されることになる。

【0080】この場合、「メッセージ表示」の保全処理はコード番号により複数の使い分けが可能である。例えばコード番号により「所有者連絡先」、「住所」、「電話番号」、「拾得者へお願い」、「拾得者へのお礼内容」など、所有者が盗難や紛失された場所や場合によってメッセージを使い分けができる。例えば「拾得者へお願い」の場合は『この装置を拾って頂いた方は、お手数ですが次にご連絡頂きますようお願い致します。私は〇〇です。電話番号が〇〇です。よろしくお願い致します。』のメッセージ内容を表示しスピーカから呼び掛け

をする。また「拾得者へのお礼内容」の場合は『この装置を拾った方は、お手数ですが次にご連絡して下さい。謝礼に〇〇を差し上げます。電話番号が〇〇です。返却住所が〇〇です。』のメッセージ内容を表示しスピーカから呼び掛けをする。

【0081】このように本実施の形態では、盗難や紛失された携帯型電子装置の所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示部に表示すること、またはスピーカから呼び掛けをすることにより、拾得者が所有者に連絡をすることができれば、所有者に返還させることができる。また、拾得者が使用するたびに返却要求のメッセージで訴えたと、拾得者が使用することを回避させることができる。

【0082】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【0083】特に、本実施の形態では、装置の拾得者にメッセージ表示により装置の返却を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、所有者に返還できる効果がある。

【0084】（実施の形態8）本発明の実施の形態8における保全処理手段の保全処理内容dについて、図10を参照して説明する。

【0085】保全処理内容dは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に蓄積記憶した連絡先にのみ発信する「所有者連絡発信」の保全処理である。例えば、盗難や紛失された携帯型電子装置の所有者が予め契約した警備会社の連絡先を登録しておけば、拾得者が無断使用しようとしてダイヤルした場合にも、警備会社の連絡先にすべて発信する。

【0086】図10は携帯型電子装置の本来の機能を停止するための「所有者連絡発信」の保全処理ルーチンを示すフローチャートである。まず、ステップS301において「所有者連絡発信」フラッグがオンかを判定し、「所有者連絡発信」フラッグがオンでない場合はステップS302に進み、「所有者連絡発信」の保全処理を実行しない。また、「所有者連絡発信」フラッグがオンである場合はステップS303に移行して、予め設定した連絡先の内容を記憶手段から選択し、記憶した所定の連絡先1を表示部に表示する（ステップS304）。そして、記憶した所定の連絡先1に自動発信・接続し（ステップS304A）、所有者連絡発信の保全処理を実施する（ステップS307）。

【0087】また、別の連絡先内容を選択した場合は、記憶した所定の連絡先2を表示部に表示する（ステップS305）。そして、記憶した所定の連絡先2に自動発信・接続し（ステップS305A）、所有者連絡発信の

保全処理を実施する（ステップS307）。

【0088】このように「所有者連絡発信」の保全処理のルーチンでは、所有者連絡発信フラッグをオンすると事前に記憶した所定の連絡先にのみ発信可能になる。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者連絡発信フラッグのオンを確認し、所定の連絡先に優先的に発信が移行する。したがって、所有者が予め所有者自身を連絡先に登録した場合は、所有者は拾得者と必ず発信ができ、拾得者に直に返却の依頼ができる。また、この場合、拾得者は所有者以外への発信使用することができないから、盗難にあった場合でも第3者は使用することができず、回線使用料金が無謀に請求されることがない。

【0089】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【0090】特に、本実施の形態では、装置の拾得者の使用に対し所有者連絡発信により連絡が取れ装置の返却を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、所有者に返還できる効果がある。

【0091】（実施の形態9）本発明の実施の形態9における保全処理手段の保全処理内容eについて、図11を参照して説明する。

【0092】保全処理内容eは、盗難や紛失された携帯型電子装置の本来の機能のうちを所有者があらかじめ入力した機能を停止する「発信機能禁止」の保全処理である。装置の本来の機能のうち例えば、ダイヤル入力機能を停止することにより発信通話を禁止したり、記録機能のみを停止することにより所有者に関する個人情報だけをセキュリティ保護するなど部分的な機能のみを保全処理する。

【0093】図11は携帯型電子装置の本来の機能を停止するための「発信機能禁止」の保全処理ルーチンを示すフローチャートである。まず、ステップS281において「発信機能禁止」フラッグがオンかを判定し、「発信機能禁止」フラッグがオンでない場合はステップS282に進み、「発信機能禁止」の保全処理を実行しない。また、「発信機能禁止」フラッグがオンである場合はステップS283に移行して、発信要求コード番号を無効にする発信機能をオフし、発信機能禁止の保全処理を実施する（ステップS284）。

【0094】このように「発信機能禁止」の保全処理ルーチンでは、発信機能禁止フラッグをオンすると発信通話を禁止する。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、発信機能禁止フラッグがオンを確認し、発信通話の禁止へ優先的に移行する。したがって、拾得者は発信通話ができず他人への

交信使用することができず、盗難に遭遇した場合でも第3者に使用されることがなく、回線使用料金が所有者に無謀に請求されることがない。

【0095】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【0096】特に、本実施の形態では、装置の拾得者の使用に対し発信機能禁止の保全処理により、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【0097】（実施の形態10）本発明の実施の形態10における保全処理手段の保全処理内容fについて、図12を参照して説明する。

【0098】保全処理内容fは、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理である。例えば、携帯型電子装置の所有者に関する個人情報や内部機密データを特定な記憶指定ロックで保管し、予め指定したキーワード以外の手順では開示できないようにする。

【0099】図12は携帯型電子装置の本来の機能を停止するための「データ出力禁止」保全処理のルーチンを示すフローチャートである。まず、ステップS341において「データ出力禁止」フラグがオンかを判定し、「データ出力禁止」フラグがオンでない場合はステップS342に進み、「データ出力禁止」の保安処理を実行しない。また、「データ出力禁止」フラグがオンである場合はステップS343に移行して、発信要求コード番号を無効にする発信機能のオフ内容を選択し、データ出力禁止の保全処理を実施する（ステップS344）。

【0100】このように「データ出力禁止」の保全処理ルーチンでは、データ出力禁止フラグをオンするとデータ出力を禁止する。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、データ出力禁止フラグがオンを確認し、データ出力を禁止する処理に優先的に移行する。したがって、拾得者や第3者はデータを出力できず、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。また、盗難や紛失された後「データ出力禁止」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎなく、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。

【0101】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【0102】特に、本実施の形態では、装置の内部の個人データや情報を保護するデータ出力禁止の保全処理により、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【0103】（実施の形態11）本発明の実施の形態11における保全処理手段の保全処理内容gについて、図13を参照して説明する。

【0104】保全処理内容gは、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理であり、携帯型電子装置の記録部の所有者に関する個人情報やデータを消去し、他人の開示を回避する。

【0105】図13は携帯型電子装置の本来の機能を停止するための「記憶データ消去」の保全処理ルーチンを示すフローチャートである。まず、ステップS321において「記憶データ消去」フラグがオンかを判定し、「記憶データ消去」フラグがオンでない場合はステップS322に進み、「記憶データ消去」の保安処理を実行しない。また、「記憶データ消去」フラグがオンである場合はステップS323に移行して、記憶手段の所定のエリアのデータを消去し、記憶手段のユーザーエリアのデータ（個人情報、装置の固有情報、通話番号等）の選択を禁止する。その後、記憶データ消去の保全処理を実施する（ステップS324）。

【0106】このように「記憶データ消去」の保全処理ルーチンでは、記憶データ消去フラグをオンすると記憶データが消去される。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、記憶データ消去フラグがオンを確認し、記憶データを消去する処理に優先的に移行する。したがって、拾得者や第3者が盗難や紛失された携帯型電子装置を使用としても記憶データ消去されており、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。また、盗難や紛失された後「記憶データ消去」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎず、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。

【0107】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【0108】特に、本実施の形態では、装置の内部の個人データや情報を保護する記憶データ消去の保全処理で、装置の紛失者にとって他人に使用されることを防止し不当な使用に伴う料金が生じることを回避し、個人データや情報を他人に悪用されることを阻止できる効果がある。

【0109】（実施の形態12）本発明の実施の形態12における保全処理手段の保全処理内容hについて、図14を参照して説明する。

【0110】保全処理内容hは、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理であり、他人に悪用され通話料金の請求を回避する。

【0111】図14は携帯型電子装置の本来の機能を停止するための「通信回線番号消滅」の保全処理ルーチンを示すフローチャートである。まず、ステップS361において「通信回線番号消滅」フラッグがオンかを判定し、「通信回線番号消滅」フラッグがオンでない場合はステップS362に進み、「通信回線番号消滅」の保安処理を実行しない。また、「通信回線番号消滅」フラッグがオンである場合はステップS363に移行して、通信ダイヤルスイッチディスエーブルフラッグをオンする。そして、ステップS364で携帯型電子装置の電源を強制的にオフし、通信回線番号消滅の保全処理を実施する（ステップS365）。

【0112】このような「通信回線番号消滅」の保全処理ルーチンでは、通信回線番号消滅フラッグをオンすると記憶された携帯型電子装置の通信回線番号を消滅される。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、通信回線番号消滅フラッグがオンを確認し、携帯型電子装置に記憶された通信回線番号を消去する処理に優先的に移行する。したがって、拾得者や第3者が盗難や紛失された携帯型電子装置を使用としても記憶されていなければならない通信回線番号が消滅され、他人が全く利用することができない。また、盗難や紛失された後「通信回線番号消滅」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎなく、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。また、通信回線番号は、携帯型電子装置の製造者または販売者のみが特殊な方法で入力することができ、電源をオフしても登録内容が保持される内部記憶媒体部に1度だけ記憶された各装置の固有の番号である。

【0113】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることによる所有者が害を被ることを排除する所定のセキュリティを高める効果がある。

【0114】特に、本実施の形態では、装置の拾得者の使用に対し通信回線番号を消滅させて発信機能を不可能にする保全処理であるから、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる 果がある。

【0115】（実施の形態13）本発明の実施の形態1

3における保全処理手段の保全処理内容iについて、図15を参照して説明する。

【0116】保全処理内容iは、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理であり、携帯型電子装置の記録部の所有者に関する個人情報やデータを他の所定の電子装置に転送し、その後、該装置の記録部の個人情報やデータを他の所定の電子装置が流用する。

【0117】図15は携帯型電子装置の本来の機能を停止するための「記憶データ転送」の保全処理ルーチンを示すフローチャートである。まず、ステップS381において「記憶データ転送」フラッグがオンかを判定し、「記憶データ転送」フラッグがオンでない場合はステップS382に進み、「記憶データ転送」の保安処理を実行しない。また、「記憶データ転送」フラッグがオンである場合はステップS383に移行して記憶手段から記憶データを読み出し、記憶データを送信する（ステップS384）。その後、データ転送が完了したかを判定する（ステップS385）。ここで、データ転送が完了しない場合はステップS383に戻り、データ転送が完了した場合はステップS386に移行して記憶部を破壊しデータを消去する。そして、記憶データ転送の保全処理を実施する（ステップS387）。

【0118】このように「記憶データ転送」の保全処理ルーチンでは、記憶データ転送フラッグをオンすると記憶データを転送し回収される。これにより、盗難や紛失された携帯型電子装置に記憶させた個人情報やデータを読み取り転送させることができ、更にその後装置の記録手段の記憶データを消去する処理に優先的に移行する。したがって、携帯型電子装置を盗難や紛失された時に本保全処理により、所有者は他の所定の電子装置に記憶データを読み取り転送し回収でき、その後で元の記憶データを消去できるため、拾得者や第3者が盗難や紛失された携帯型電子装置を使用としても記憶データは消去されており、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。

【0119】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例えば携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることによる所有者が害を被ることを排除する所定のセキュリティを高める効果がある。

【0120】特に、本実施の形態では、装置の内部の個人データや情報を遠隔操作で転送する「記憶データ転送」の保全処理により、装置の紛失者にとって他人に使用される前に内部の個人データや情報を転送回収して、その後装置内部の記憶データを消去し、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【0121】（実施の形態14）本発明の実施の形態14における保全処理手段の保全処理内容について、図16を参照して説明する。

【0122】保全処理内容iは、使用者を識別し、所有者以外の他人が携帯型電子装置を使用を不可能にする「使用者の識別」の保全処理である。使用者の識別は、例えばパスワード入力、指紋認識、声紋認識など使用者の識別手段により、所有者以外の人が携帯型電子装置を使用した時に保全処理が実行される。

【0123】図16は携帯型電子装置の本来の機能を停止するための「使用者の識別」の保全処理ルーチンを示すフローチャートである。まず、ステップS401において「使用者の識別」フラグがオンかを判定し、「使用者の識別」フラグがオンでない場合はステップS402に進み、「使用者の識別」の保安処理を実行しない。また、「使用者の識別」フラグがオンである場合はステップS403に移行して装置の発信通話機能を先ずオフし、次いで使用者識別番号かを判定する（ステップS404）。ここで、使用者識別番号でない場合はステップS402に戻り、使用者識別番号の場合はステップS405、ステップS406、ステップS407のいずれかへ移行して使用者の識別を行う。

【0124】使用者の識別の一つは、使用時にパスワードの入力を要求し、この入力パスワードと携帯型電子装置の所有者が予め設定し登録したパスワードと比較し（ステップS405）、パスワードが一致したかを判定する（ステップS405A）。ここで、一致した場合はステップS409に移行して正常使用を可能にする。また、不一致の場合は、パスワードの誤入力に対するリトライ回数を3回に定め（ステップS405B）、パスワードの誤入力力が3回以上あった場合は更に強度の保全処理を実行する（ステップS408）。この時の所有者が予め設定するパスワードは、電源をオフしても登録内容が保持される記憶部に1度だけ記憶する。使用前にパスワードの入力してから運用する保全処理は従来もあったが、通常時には厄介なこともあり平常はその保全処理を解除していることが多い。しかし本保全処理は、携帯型電子装置の所有者が、その携帯型電子装置が盗まれたり紛失した場合に、保全を要する携帯型電子装置に遠隔操作データを送信し、パスワードによる保全処理の機能を働かさせるところに特徴を有する。

【0125】また、使用者の識別の他の例としては、携帯型電子装置を使用する者に指紋の入力を要求し、この指紋と携帯型電子装置の所有者が予め設定し登録した指紋とを比較し（ステップS406）、指紋が一致したかを識別する（ステップS406A）。ここで、使用者の指紋入力する場合は、例えば携帯電話機を持つ手の親指が当たる部分に指紋を検出する機能と指紋を認識する機能を付加することで可能になる。したがって、指紋の一致が認識された場合はステップS409に移行して正常

使用を可能にする。また、指紋の不一致が認識された場合は、指紋の誤入力に対するリトライ回数を3回に定め（ステップS406B）、指紋の誤入力力が3回以上あった場合は更に強度の保全処理を実行する（ステップS408）。

【0126】また、使用者の識別の更に他の例としては、パスワードを音声化し、予め登録したパスワードの音声データ（声紋）とマイクから入力した声紋を照合し（ステップS407）、声紋が一致したかを認識する（ステップS407A）。ここで声紋の一致が認識された場合はステップS409に移行して正常使用を可能にする。また、声紋の不一致が認識された場合は、声紋の誤入力に対するリトライ回数を3回に定め（ステップS407B）、声紋の誤入力力が3回以上あった場合は更に強度の保全処理を実行する（ステップS408）。

【0127】このように「使用者の識別」の保全処理ルーチンでは、使用者の識別フラグをオンすると使用者の識別手段によりパスワード、指紋、声紋を識別し、所有者以外の人が携帯型電子装置を使用を検出した場合には使用者の識別フラグがオンを確認し、装置の発信通話を禁止する処理に優先的に移行する。したがって、拾得者は発信通話ができず他人への交信使用することができない。

【0128】他の保全処理のうち1つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されることを排除する所定のセキュリティを高める効果がある。

【0129】（実施の形態15）次に、本発明の請求項15に対応する実施の形態15の保全処理について説明する。この実施の形態による保全処理内容は、次に示す内容から構成される。

【0130】保全処理内容aは、携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理であり、送信した相手に、個人情報やデータを所有者が受信できない事情にある旨を知らせ、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されることを保全する。

【0131】保全処理内容bは、携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理であり、他人の拾得者に個人情報やデータが漏洩されないように、相手からの受信情報を受信する機能を停止し保全する。

【0132】保全処理内容cは、携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理であり、送信した相手が、個人情報やデータを所有者に送信する前に話中または使用中の信号データを一方的に送信して、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されるこ

とを保全する。

【0133】保全処理内容dは、携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理であり、送信した相手が、個人情報やデータを所有者に送信する前に通信手続きの動作において、例えばアクセス信号を送信せずに、送信情報を送信する機能を停止し、交信を回避する。

【0134】保全処理内容eは、携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理であり、保全処理内容cにおける話中または使用中の信号データの代わりに、予め入力して記憶手段に蓄積記憶した紛失メッセージを一方向的に送信して、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されることを保全する。

【0135】保全処理内容fは、携帯型電子装置に送信した相手に、該携帯型電子装置の使用を防止する保全処理であり、他人の拾得者が拾得した携帯型電子装置を使用した個人情報やデータを、所有者の個人情報やデータとして相手が交信したことによる問題を回避するために、転送先を固定し記憶された住所など消去するもので、他人の開示を回避する。

【0136】以上の保全処理のうち1つ以上の処理を実施する結果により、例え携帯型電子装置を盗まれたり紛失しても、その装置の所有者に送信した相手にとって、携帯型電子装置の個人データの保護や他人に使用されて所有者が害を被ることが排除され、所定のセキュリティを高めることができる。

【0137】（実施の形態16）次に、本発明の請求項16に対応する実施の形態16の保全処理について説明する。この実施の形態は、電波通信手段を伝送媒体とし、所有者が予め入力して記憶手段に蓄積記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全機能を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたところにある。

【0138】図1において、携帯型電子装置1を盗まれたり紛失した所有者は、一般公衆電話や携帯電話としてのPHSなど電話機3を操作して携帯型電子装置1に電話をかける。この場合市内や市外の一般公衆電話3Aから公衆回線網2cを介して、またPHSデータ通信装置や携帯電話としてのPHS3から無線通信回線2bを介して保全を要する携帯型電子装置1に遠隔操作データを送信する。

【0139】次に、本実施形態の保全処理動作について図17に示す保全確認のルーチンを用いて説明する。

【0140】盗難や紛失した携帯型電子装置1は、多くの場合に他人が拾得していることがあり、通話が可能である。次に携帯型電子装置1を盗まれたり紛失した所有者は、所有者が予め入力して記憶手段に蓄積記憶した

キーワード信号を送信する。記憶手段に蓄積記憶したキーワード信号を受信した場合に、該携帯型電子装置1は遠隔操作データを受信する受信部11で受信し（ステップS171）、受信した遠隔操作データが予め記憶された所定のキーワード信号と一致することを識別する識別部12で判定する（ステップS172）。識別部12の識別結果により一致が確認された場合のみ保全確認信号を発信する（ステップS173）。この保全確認信号の指示により他の機能を強制的にオフし（ステップS174）、次いで保全部13が強制的に携帯型電子装置の保全機能を駆動し（ステップS175）、携帯型電子装置の所有者が害を被ることを排除する所定の保全処理をするように動作する。

【0141】特に、本実施の形態では、装置の紛失者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信し、強制的に携帯型電子装置の保全機能を駆動し、装置の紛失者にとって他人に使用されることを防止できる。

【0142】（実施の形態17）次に、請求項17に対応する実施の形態17について、図18を参照して説明する。この実施の形態では、所有者が予め入力して記憶手段に蓄積記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の接続を行い、所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたものである。

【0143】すなわち、第1回目の受信の呼び出し信号回数をカウントし（ステップS101）、そのカウント値が予め設定した第1回目のコール回数と識別したかを判定する（ステップS182）。ここで、否定判定された場合はステップS181に戻り、肯定判定された場合はステップS183に進む。ステップS183では、第2回目の受信の呼び出し信号回数をカウントし、そのカウント値が予め設定した第2回目のコール回数と識別したかを判定する（ステップS184）。ここで、否定判定された場合はステップS181に戻り、肯定判定された場合はステップS185に進む。

【0144】ステップS185では、第3回目の受信の呼び出し信号回数をカウントし、そのカウント値が予め設定した第3回目のコール回数と識別したかを判定する（ステップS186）。ここで、否定判定された場合はステップS181に戻り、肯定判定された場合はステップS187に進む。ステップS187では保全システムを立ち上げ、次の受信の呼び出し信号回数から保全内容を識別したかを判定する（ステップS188）。保全内容を識別した場合はステップS189に進み、遠隔操作データの保全内容を解析する。そして、遠隔操作データの識別結果に応じた保全処理を実施する（ステップS190）。

【0145】このように盗難や紛失した携帯型電子装置

を拾得した者が応答したとか、交信ができない事態の場合においても、予め入力して記憶手段に蓄積記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により強制に電源供給を中断し、即停止するなどの所定の保全処理内容を適用するように動作する。

【0146】上記の呼び出し信号回数のパターンは、例えば第1回目の10回呼び出し後一旦フック回線をオフし、第2回目の5回呼び出し後一旦フック回線をオフし、第3回目の8回呼び出し後一旦フック回線をオフするものであり、この呼び出し信号回数のパターンを所定時間の期間に繰り返すパターンを受信した場合に、所定の保全処理内容を適用する。

【0147】なお、本発明の請求項8は、実施の形態4における携帯型電子装置の遠隔操作データの処理ルーチンで、図6のステップS20、ステップS21によるキーワード識別に相当する遠隔操作か否かを識別する方法を代替えるものである。その結果により個々の保全処理の内容については、上記と同様のため説明を省略する。

【0148】本実施の形態による保全処理は、携帯型電子装置を情報携帯端末電話装置に適用した実例であるが、一般的な情報携帯端末機やPHSやコードレス電話機においても適用できるものである。

【0149】特に、本実施の形態では、装置の拾得者が応答しなとか、交信ができない事態の場合においても、呼び出し信号回数のパターンによる遠隔保全処理を起動させ、装置の紛失者にとって他人に使用されることを防止できる。

【0150】（実施の形態18）次に、本発明の請求項18に相当する実施の形態18の携帯型電子装置保全システムについて図19を参照しながら説明する。

【0151】この実施の形態では、携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置保全システムである。特に微弱電波或いは超音波などを用いた子機を備えた携帯型電子装置に関するもので、実施の形態1のように、この種の携帯型電子装置はいつか如何なる時でも遺失の件数は膨大し、小型携帯上は優れており便利であるが盗難に合いやすい。これらの遺失対策はそれらの所有者が細心の注意を払う以外にないが、それが如何に効果の少ない方法であるかを多く体験していることである。

【0152】この問題を解決する手段として本実施の形態では、微弱電波或いは超音波或いは誘導電波などを発振する発振手段と、それを本体に送信する微弱電力送信手段を有する子機を備え、該子機からの保全処理を促すための発振データを受信する手段、受信した操作データを識別する手段、該識別の結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を備えてた携帯型電子装置（本体）で構成し、上記微弱電力送

信手段を有する子機は、鎖付きのペンダントやピアスのように身近に携帯する小型軽量が望まれる。子機は、服装のポケットなどにしっかりと挿入できるようにフックやベルト付きにし、またはピアスやペンダントに内蔵し子機自身の紛失を防ぐものである。

【0153】本体の携帯型電子装置は子機からの保全処理を促すための発振データを受信する受信手段を有し、該受信した操作データを識別する手段で、所定の保全手段を動作するものである。また前記微弱電力送信手段の送信する信号が該受信手段に着信する距離を例えば数メートル程となるように設定し、その通信可能距離以上に上記送受信手段、すなわち本体と子機との両者が離れると着信信号レベルが所定以下になり、該受信した操作データを識別する手段は、本体の携帯型電子装置が所定の距離以上に所有者から離れた、即ち所有者が本体の携帯型電子装置を置き忘れたか遺失したものと識別する。そして該識別の結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を動作させる。保全手段は、例えば所有者にその旨を気付かせるように警告する警告ブザーを鳴らすことや、携帯型電子装置本体に保全処理を促すための前記実施の形態1のように各種の保全機能を起動させる。

【0154】図19は、本実施の形態18の一例を示す構成図である。同図において、子機における発振器21からの出力信号を伝送部22で変調増幅し、微弱電力送信手段23からアンテナを通して所定の微弱電力信号を送信する。

【0155】一方、該信号を本体のアンテナから微弱電力受信部24で受信する。受信信号は伝送部25で復調増幅され、検波部26により検波した後、その受信レベルが予め設定したレベル以下かどうかを判定部27で判別し、受信のレベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する。子機と本体との空間間距離が所定の距離に比べて離れると本体に保全処理を促すための各種の保全処理を行う保全手段28が動作し、例えば所有者にその旨を気付かせるように警告ブザーを鳴らす。

【0156】上記のように、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本システムが作動して未然に紛失または置き忘れを防止し回避することができる。また所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【0157】（実施の形態19）図20は、本発明の請求項19に対応する実施の形態19の構成を示す機能ブロック図である。同図において、子機は発振器41、発振器41からの出力信号を変調増幅する伝送部42、伝送部42からの信号を本体へ送信するとともに本体から

の信号を受信する微弱電力伝送手段43、微弱電力伝送手段43の受信信号を復調増幅する伝送部44、復調信号を検波する検波部45、検波信号の受信レベルが予め設定したレベル以下かどうかを判別し、かつ受信レベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する判定部46、子機保全のための各種の保全処理を行う保全手段47、信号の交信をリセットするリセット部48から構成されている。

【0158】また、本体は子機からの信号を受信するとともに子機へ進行を送信する微弱電力伝送手段49、微弱電力伝送手段49の受信信号を復調増幅する伝送部50、復調信号を検波する検波部51、検波信号の受信レベルが予め設定したレベル以下かどうかを判別し、かつ受信レベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する判定部52、本体保全のための各種の保全処理を行う保全手段53、信号の交信をリセットするリセット部54、発振器55、発振器55からの出力信号を変調増幅して微弱電力伝送手段49へ出力する伝送部56から構成されている。

【0159】この構成において、図19に示した場合と同様に形態型電子装置の本体と子機間の距離が、例えば数メートル程度離れることで通信可能距離以上になると着信信号レベルが所定以下になり、該受信した操作データを識別する判定部46及び52は、本体の携帯型電子装置が所定の距離以上に所有者から離れた、即ち所有者が本体の携帯型電子装置を盗難および置き忘れたか遺失したものと識別すると、その識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段47及び53が動作を開始し、未然に盗難および紛失または置き忘れを防止し回避することができる。保全手段47及び53は、例えば所有者にその旨を気付かせるように警告する本体及び子機の一方または双方で警告ブザーを鳴らすことや、携帯型電子装置本体に保全処理を促すための前記実施の形態のように各種の保全機能を起動させる。

【0160】このように本体及び子機に警告を発生する手段を有することによって、所有者が携帯型電子装置を盗難および紛失または置き忘れそうになった場合に、本システムの保全手段が作動して未然に盗難および紛失または置き忘れを防止し回避することができる。特に盗難および置き引きに遭遇した場合に、警告音を発生することの効果や危険性を考慮し、子機から警告音を発生させずバイブレーションで所有者に報知することで周囲の人々に気付かれないで紛失または置き忘れを回避できる。また、警告音を発生させて周囲の人々に気付かせたいのか、または周囲の人々に気付かれないで解決するか切り替えることができる。

【0161】更に、子機に着信信号レベルを換算し本体と子機との両者間の距離を表示する機能を設ける携帯型電子装置においては、所有者が携帯型電子装置を紛失ま

たは置き忘れそうになった場合に、本体と子機との両者間の距離を表示する子機により、本体の存在する位置を検索することができる。例えば部屋内で本体を見失った場合に、子機と本体間の距離の表示の変化で本体が存在する位置を見つけ出すことが可能になる。

【0162】また、上記の本実施の形態において、信号の交信をリセットするリセット部を付加することが運用上便利である。リセット部を付加することは、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に動作した後、再度本実施例の機能を運用させる上で極めて大きい効果を有する。

【0163】上記の説明により本発明のように携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置の保全システムを容易に実施することができ、携帯型電子装置を紛失または置き忘れを防止する上で大きな効果を有する。

【0164】なお、上記実施の形態における保全処理は携帯型電子装置を情報携帯端末電話装置に適用した場合について説明したが、一般的な情報携帯端末機やPHSやコードレス電話機においても適用できるものである。

【0165】

【発明の効果】以上のように本発明の携帯型電子装置の保全システムによれば、上記実施例より明らかなように、以下の効果を得ることができる。

【0166】携帯型電子装置（PHS、携帯電話機も含む電波通信手段を有するデータ処理端末装置）の盗難や紛失に対して、その所有者が遠隔操作するところにより、携帯型電子装置の所有者が害を被ることを排除する所定の保全手段が動作し、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることができる。すなわち、簡単に携帯型電子装置の内部のデータを保護することができ、更に他人に使用されても料金を支払うという不具合を回避することができる。

【0167】また、所有者が携帯型電子装置の盗難や紛失に気が付いた場合に、所有者が積極的に保全を要求することにより、携帯型電子装置の所有者に不利益となる要因を防止することができる。即ち、携帯型電子装置の記憶内部および仕様に関してプロテクトをかけて保護することができる。

【0168】また、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思ってに送信したことで、送信相手または相手情報が害を被る問題が発生するという不具合を回避することができる。即ち、盗難や紛失した携帯型電子装置の所有者や送信相手が害を被ることを排除することができる。

【0169】また、本発明の携帯型電子装置の保全システムによれば、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本システムが作動して未然に紛失または置き忘れを防止し回避することができるほ

か、所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【図面の簡単な説明】

【図 1】本発明の実施の形態 1 における携帯型電子装置の保全システムの概略構成図

【図 2】本発明の実施の形態 2 における携帯型電子装置の保全システムの構成を示す機能ブロック図

【図 3】本発明の実施の形態 2 におけるプロトコールのハードウェア構成図

【図 4】本発明における携帯型電子装置のネットワークシステムを示す図

【図 5】本発明におけるセキュリティを高める保全処理の制御ルーチン図

【図 6】本発明における遠隔操作データの処理ルーチン図

【図 7】本発明における電源オフの保全処理ルーチンを示すフローチャート

【図 8】本発明における警告発生の保全処理ルーチンを示すフローチャート

【図 9】本発明におけるメッセージ表示の保全処理ルーチンを示すフローチャート

【図 10】本発明における所有者連絡発信の保全処理ルーチンを示すフローチャート

【図 11】本発明における発信機能禁止の保全処理ルーチンを示すフローチャート

【図 12】本発明におけるデータ出力禁止の保全処理ルーチンを示すフローチャート

【図 13】本発明におけるデータ出力消去の保全処理ルーチンを示すフローチャート

【図 14】本発明における通信回線番号消滅の保全処理ルーチンを示すフローチャート

【図 15】本発明における記憶データ転送の保全処理ルーチンを示すフローチャート

【図 16】本発明における使用者の識別の保全処理ルーチンを示すフローチャート

【図 17】本発明における保全確認のルーチンを示すフローチャート

【図 18】本発明における呼び出し信号による遠隔操作の処理のルーチンを示すフローチャート

【図 19】本発明の実施の形態 18 による携帯型電子装 *

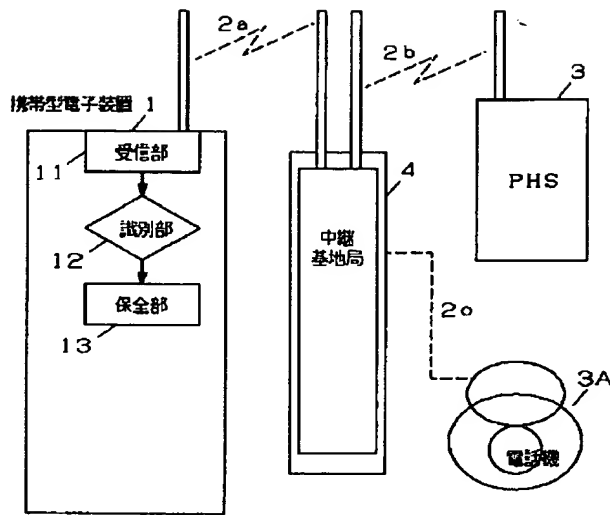
* 置の保全システムを示す構成図

【図 20】本発明の実施の形態 19 による携帯型電子装置の保全システムを示す構成図

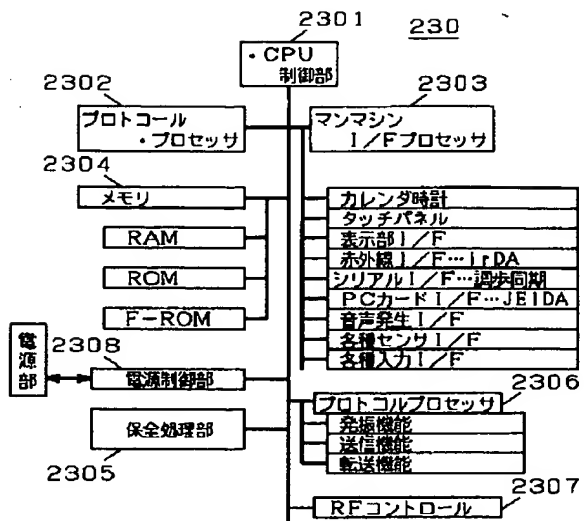
【符号の説明】

- 1 携帯型電子装置
- 2 a, 2 b, 2 c 電波通信手段
- 3 電話機 (PHS)
- 3 A 電話機
- 4 中継基地局
- 10 1 1 受信部 (受信手段)
- 1 2 識別部 (識別手段)
- 1 3 保全部 (保全手段)
- 2 1 発振器
- 2 2 伝送部
- 2 3 微弱電力送信部
- 2 4 微弱電力受信部
- 2 5 伝送部
- 2 6 検波部
- 2 7 判別部
- 20 2 8 保全手段
- 3 0 公衆ならびに専用回線網
- 3 1 一般の電話機
- 3 2 変復調器付きパソコン
- 3 3 基地局
- 3 4 基地局
- 3 5 基地局
- 3 6 網管理局
- 4 1 発振器
- 4 2 伝送部
- 30 4 3 微弱電力伝送手段
- 4 4 伝送部
- 4 5 検波部
- 4 6 判別部
- 4 7 保全手段
- 4 8 リセット部
- 4 9 微弱電力受信部
- 5 0 伝送部
- 5 1 検波部
- 5 2 判別部
- 40 5 3 保全手段
- 5 4 リセット部
- 5 5 発振器
- 5 6 伝送部

【図1】

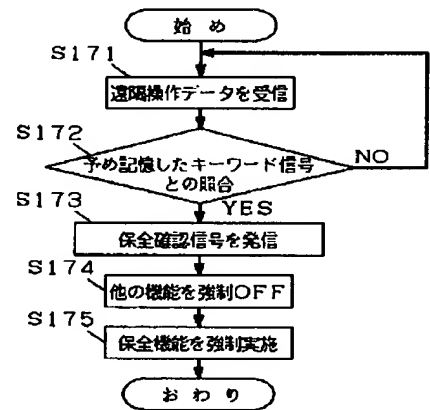
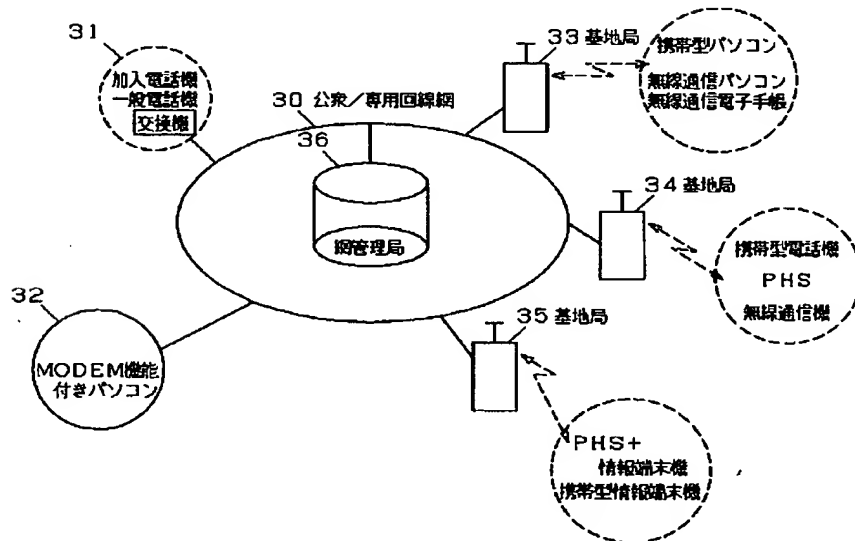


【図3】

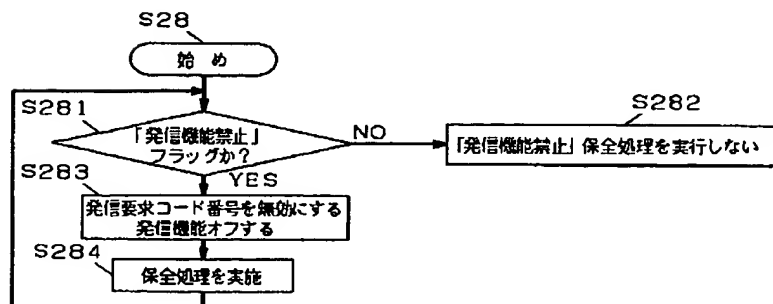


【図4】

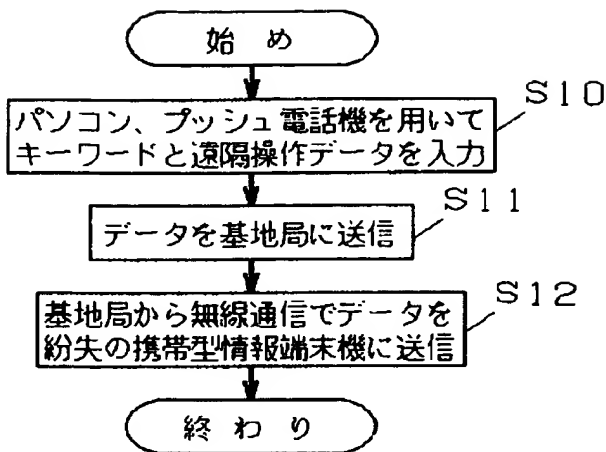
【図17】



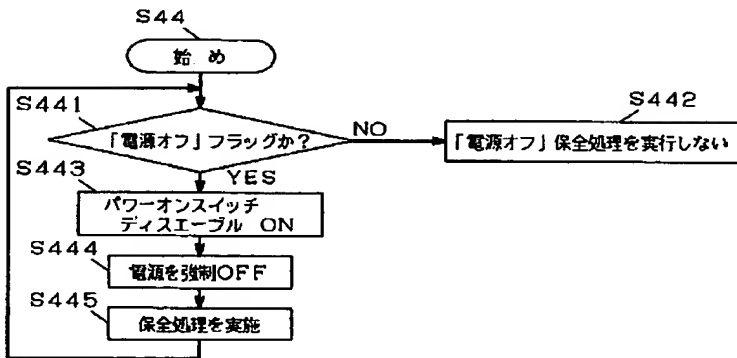
【図11】



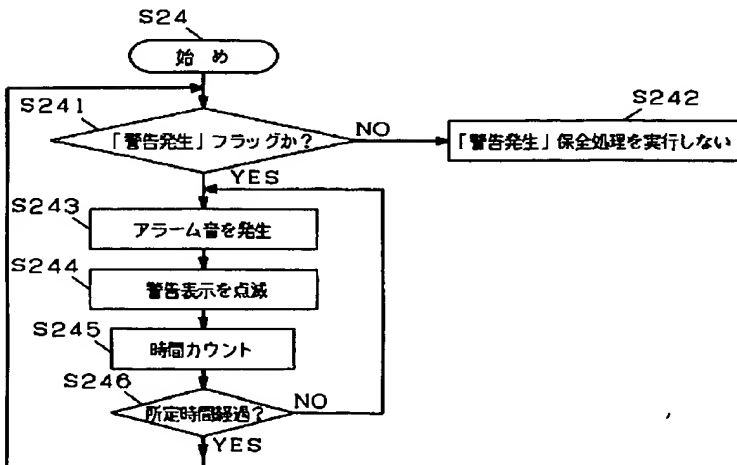
【図5】



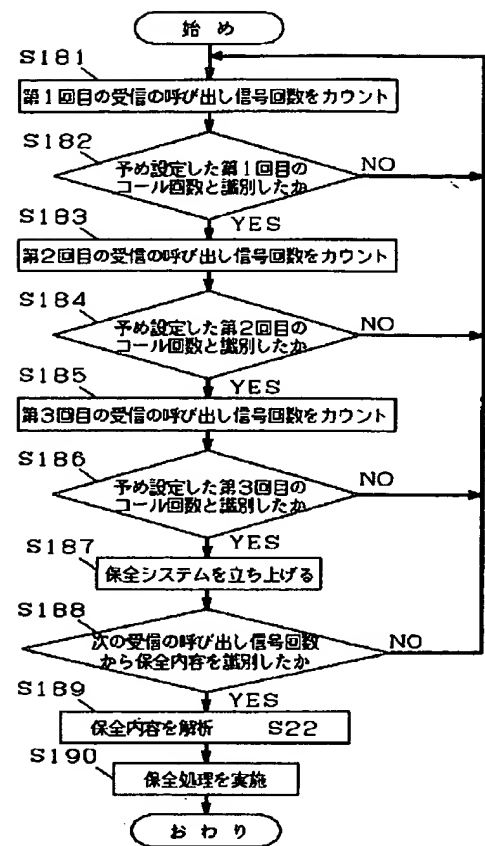
【図7】



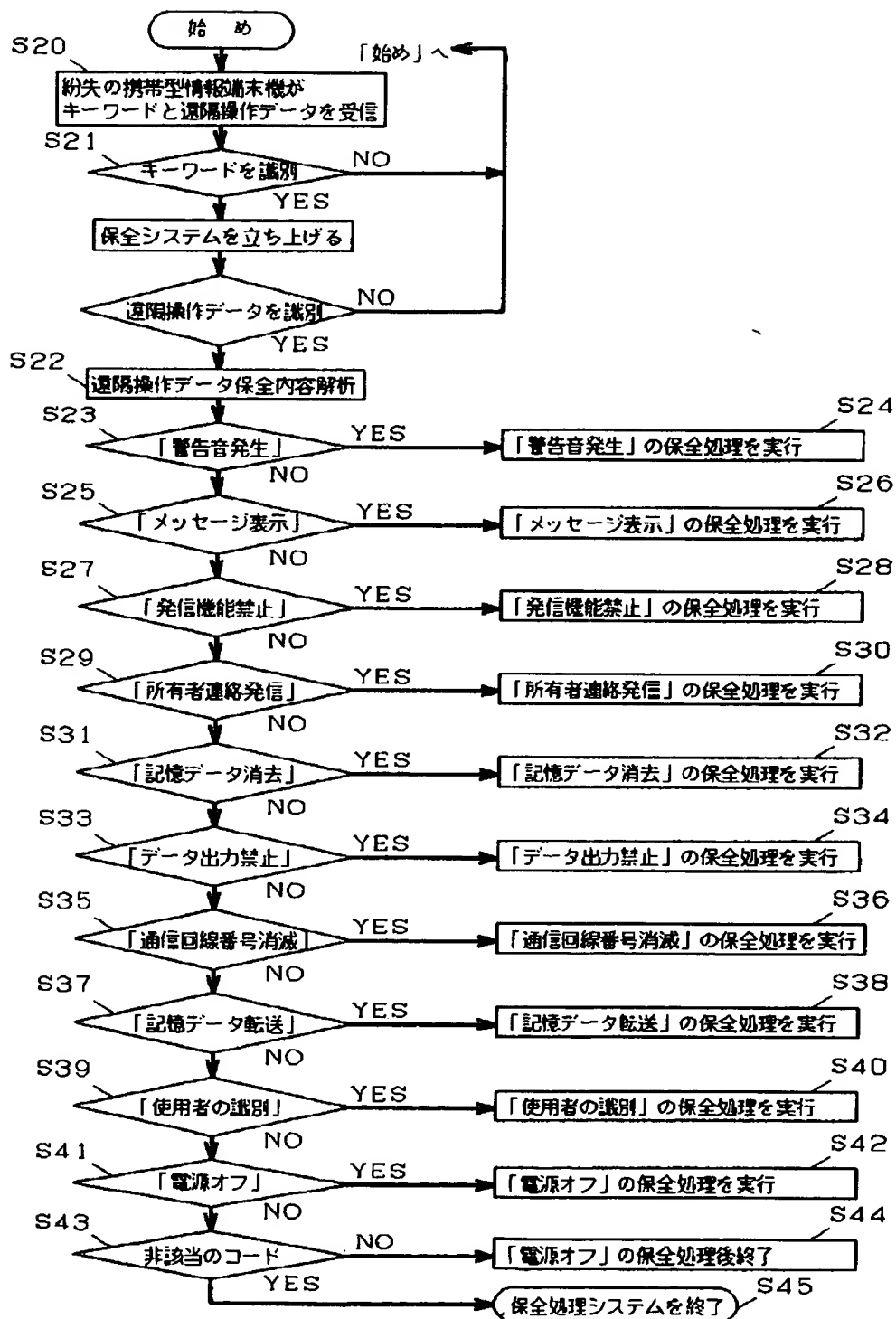
【図8】



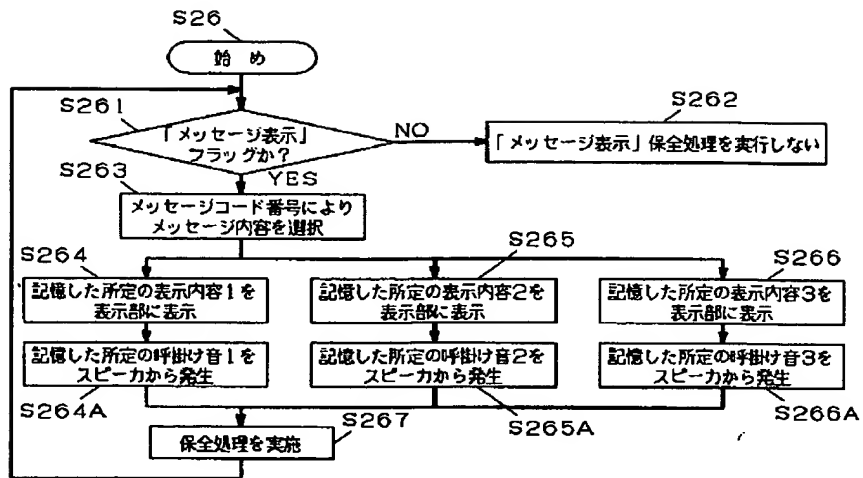
【図18】



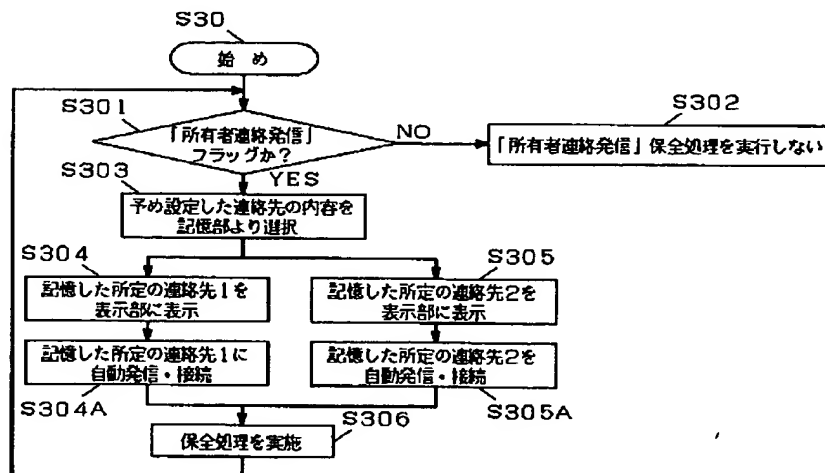
【図6】



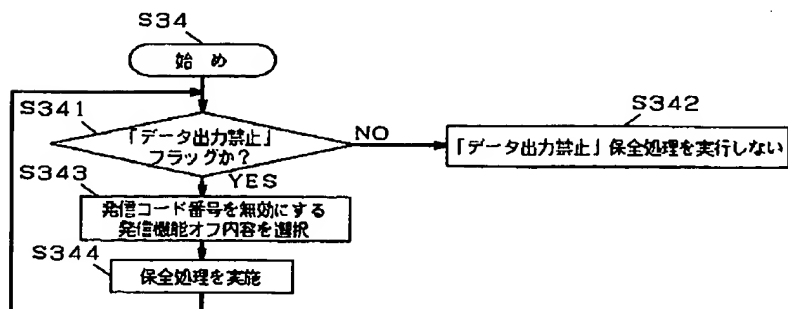
【図9】



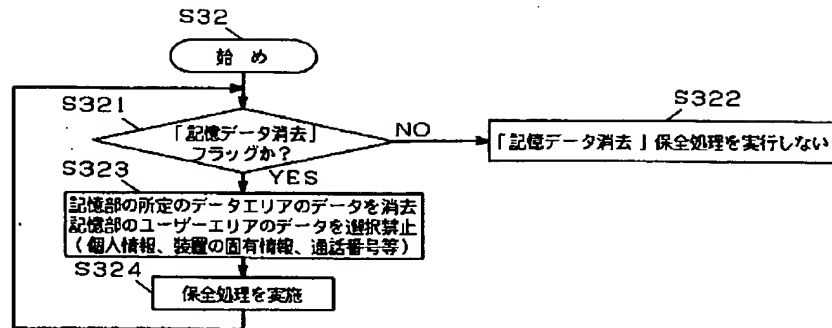
【図10】



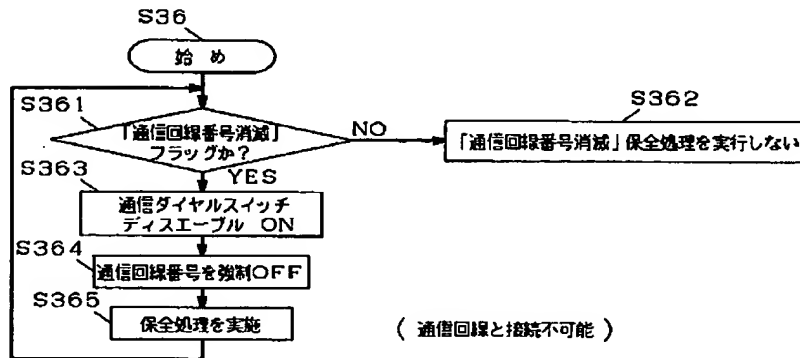
【図12】



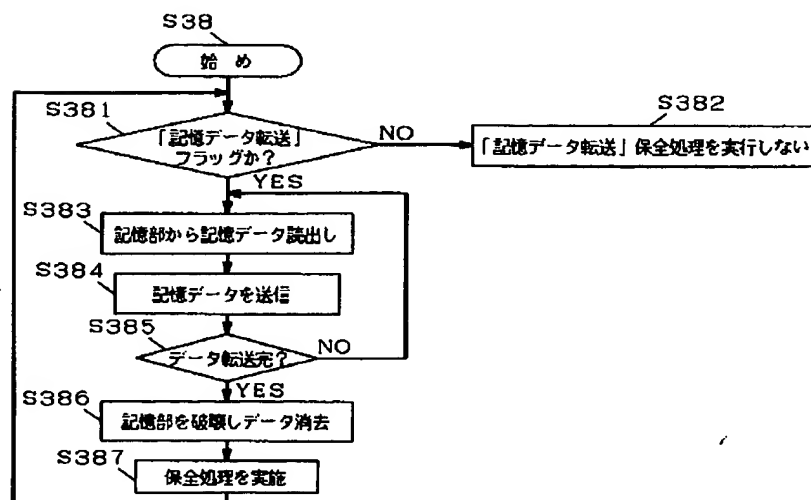
【図13】



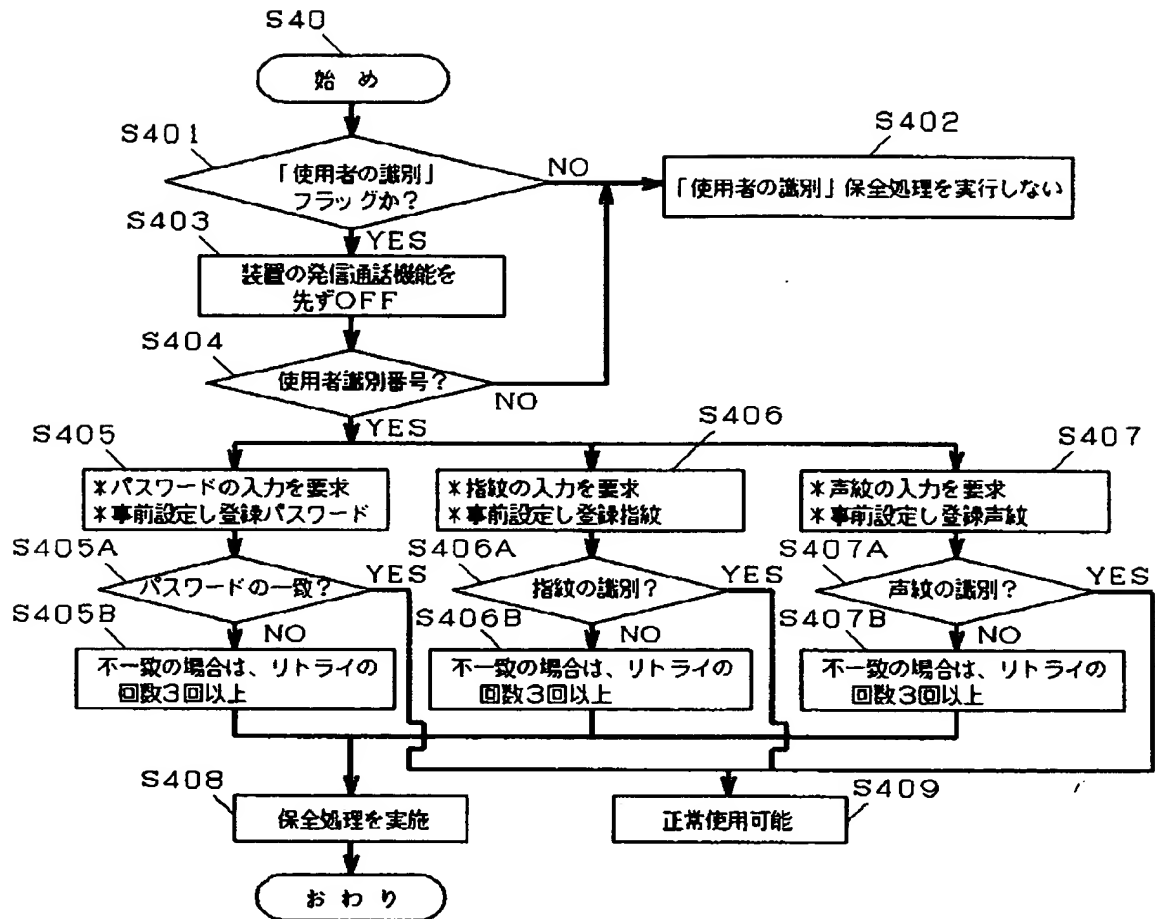
【図14】



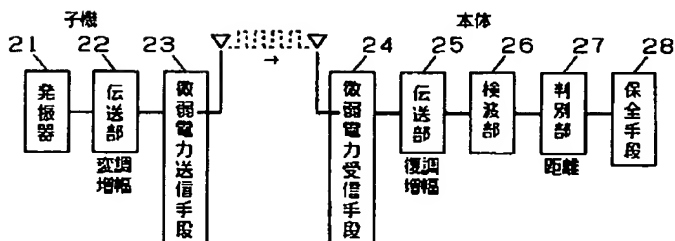
【図15】



【図16】



【図19】



【図20】

